Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (original): A system for manipulating a computer file and/or program comprising:

a serving device having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it;

a connector connected to the serving device on which the encrypted computer file and/or program travels and to which the serving device transfers the encrypted computer file and/or program; and

a client device which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program, said client device not allowing intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received, said serving device separate, apart and distinct from the client device.

Claim 2 (original): A system as described in Claim 1 wherein said server device assigns permissions and/or rights to the unencrypted computer file and/or program which identifies what

the client device can do with the unencrypted or encrypted computer file and/or program after the client device has received the encrypted computer file and/or program or after the client device has decrypted the encrypted computer file and/or program back to the unencrypted computer file and/or program.

Claim 3 (original): A system as described in Claim 2 wherein said server device encrypts the permissions and/or rights and transfers them to the client device through the connector, said client device decrypts the unencrypted permissions and/or rights.

Claim 4 (original): A system as described in Claim 3 wherein the serving device includes controlling server software and/or firmware which causes the encryption of the unencrypted computer file and/or program and the permissions and/or rights and instructs the client device to temporarily suspend user intervention when the client device receives the encrypted computer file and/or program and the encrypted permissions and/or rights.

Claim 5 (original): A system as described in Claim 4 wherein the client device includes controlling client software and/or firmware which causes the decryption of the encrypted computer file and/or program.

Claim 6 (original): A system as described in Claim 5 wherein the client device has a mechanism for requesting the unencrypted computer file and/or program from the server device.

Claim 7 (original): A system as described in Claim 6 wherein the controlling client software and/or firmware causes the encryption of the unencrypted computer file and/or program and the permissions and/or rights for storage.

Claim 8 (original): A system as described in Claim 7 wherein the client device has an operating system and the controller client software and/or firmware instructs the operating system to reestablish user intervention at a desired time.

Claim 9 (original): A system as described in Claim 8 wherein the server device has a server public key infrastructure which encrypts using encrypted communication protocols the permissions and/or rights and the unencrypted computer file and/or program.

Claim 10 (original): A system as described in Claim 9 wherein the client device has a client public key infrastructure which decrypts from transmission the permissions and/or rights and encrypted computer file and/or program using encrypted communication protocols.

Claim 11 (original): A system as described in Claim 10 wherein the client device includes an encrypting file system which encrypts the unencrypted computer file and/or program and the permissions and/or rights and allows for the manual selection of the unencrypted computer file and/or program for encryption or decryption.

Claim 12 (original): A system as described in Claim 11 wherein the client public key infrastructure has an encryption and/or decryption key and the encrypting file system uses the encryption and/or decryption key utilized by the client public key infrastructure.

Claim 13 (original): A system as described in Claim 12 including a next client device connected to the client device through the connector.

Claims 14-23 (canceled)